UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,722	03/24/1999	DAVID A. LEE	042390.P6526	1130

7590 08/03/2006

WILLIAM W SCHAAL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/275,722	LEE, DAVID A.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 remain for examination. The correspondence filed 7/10/06 cancelled claims 11-27.

Allowable Subject Matter

2. The indicated allowability of claims 1-10 is withdrawn in view of the newly discovered reference(s) to Liu. Rejections based on the newly cited reference(s) follow.

Response to Arguments

3. Applicant's arguments filed 7/10/06 with respect to the rejections of claims 1-10 over 35 USC 101 have been fully considered but they are not persuasive.

Although Examiner acknowledges that a previous rejection of claims 1-10 had been made in the Office Action of 5/27/03, the particular grounds for rejection were different: the Office Action of 5/27/03 argued a lack of utility (page 3, 2nd paragraph) whereas the current rejection argues a lack of a tangible result, in accordance with current Office practice (Office Action of 3/10/06, pages 4-5, paragraph 10).

Examiner wishes to note that Applicant has incorrectly stated in the remarks filed on 7/10/06 that claim 1 possesses a limitation reading, "dedicating the rows of the key matrix to a first classification." (amendment of 7/10/06, page 7, last line). This is incorrect; that limitation was removed in the amendment filed 5/27/05, and no such limitation is present in the claim.

With respect to Applicant's citation of *Ex Parte Lundgren*, the Examiner was not and is not alleging that there is a requirement that the steps be computer or machine implemented; and, therefore, the invention claimed here is not patent-eligible subject matter. Rather, the rejection was/is based on the lack of a tangible result of the claimed method which would allow the utility of the claimed method to be realized. As such, Applicant's argument regarding *Ex parte Lundgren* is displaced and not persuasive.

Claim Rejections - 35 USC § 101

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 1 and 11 recite a series of abstract steps in an algorithm that ultimately produces a shared secret key; however, it is clear from the disclosure that the step of "producing a shared secret key" in its broadest reasonable sense is equivalent to "calculating" and is merely performing the mathematical manipulation which formulates the result which becomes the key (specification: page 11, lines 22-24; page 13, lines 5-7; page 15, lines 14-15). It is not until the key is both produced and stored in memory or used that it becomes a tangible result which enables its usefulness in a disclosed practical application, such as securing a channel, to be realized. Examiner respectfully suggests that amending the claim to include a limitation wherein the shared secret key is subsequently used to secure a communication channel between digital platforms would be sufficient to overcome the

current rejection (specification, page 15, lines 21-23, which appears to be the only passage in the specification where an actual use for the shared secret key is taught).

Claim Rejections - 35 USC § 103

6. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech (U.S. Patent 6,118,873), and further in view of Liu (U.S. Patent 5,412,729).

Referring to Claim 11:

Lotspiech discloses a method comprising providing a key matrix having N rows and M columns, where N>2 and M>2 (Figure 3; col. 5, lines 20-41); for each [row] of the matrix, performing arithmetic operations utilizing matrix keys of at least two selected [columns] to produce a secret device key which is a part of a first set of secret device keys (col. 5, lines 42-54), and producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys (col. 5, line 55 – col. 6, line 12).

For the record, Examiner wishes to note that Lotspiech's use of the arbitrary designation "N" corresponds to Applicant's use of "M", and Lotspiech's use of the arbitrary designation "M" corresponds to Applicant's use of "N".

With respect to the limitation regarding "for each row...utilizing matrix keys of at least two columns", Lotspiech discloses wherein for at least one row the system uses keys from at least two columns ($S_{1,3}$ and $S_{1,4}$ in Figure 3), although it is not mandated that this condition be satisfied. Nevertheless, in the preferred embodiment of Lotspiech

wherein the matrix has 32 rows and 128 columns (col. 7, lines 37-39) for example, it is not only possible but highly probable (in excess of 90% likely) that following the process disclosed in col. 5, lines 42-54 will result in a scenario wherein each row of the matrix will have keys from at least two columns selected. Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to explicitly stipulate an embodiment of Lotspiech wherein for every row device keys from at least two columns are selected. The motivation for doing so would be to eliminate trivial cases (such as selecting all the keys from exactly one row) which could negatively affect the randomness of the key distribution, and by extension weaken the security of the overall system.

As was noted in the previous Office Action, Lotspiech teaches away from selecting at least two rows from each column of the matrix (col. 7, lines 47-52). However, the ability to invert a matrix (transposing rows for columns and columns for rows) to perform mathematical operations was long known in the art. As an example, Liu discloses where a matrix could be inverted (col. 8, lines 33-36) for the purpose of selecting elements from it to derive a secret key (col. 4, lines 17-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to invert Lotspiech's key matrix in a manner akin to what is disclosed by Liu. The motivation for doing so would be to facilitate encrypting data in such a way as to make it computationally infeasible for an attacker to decrypt it without knowing the secret key (Liu, col. 4, lines 1-6).

Referring to Claim 2:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 1 above. Liu further discloses the arithmetic operations include modular addition (col. 2, lines 5-10; col. 3, lines 10-12).

Referring to Claim 3:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses prior to performing the arithmetic operations, the method comprises: generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys (col. 5, lines 42-54).

Referring to Claim 4:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 3 above. Lotspiech further discloses the key selection vector is uniquely assigned to a first digital platform (col. 5, lines 52-54).

Referring to Claim 5:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 4 above. Lotspiech further discloses wherein prior to producing the shared secret key, the method comprises: receiving a key selection vector from a second digital platform in communication with the first digital platform (col. 5, lines 40-50); and analyzing contents

of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys (col. 5, lines 10-30, 40-65).

Referring to Claim 6:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses prior to performing arithmetic operations on keys of at least two selected rows, the method further comprises dedicating the rows of the key matrix to a first classification, and dedicating the columns of the key matrix to a second classification (col. 5, lines 30-40; Fig. 3; index).

Referring to Claim 7:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 6 above. Lotspiech further discloses first classification includes digital platforms designed to provide information to other digital platforms (col. 4, lines 45-65).

Referring to Claim 8:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 7 above. Lotspiech further discloses the second classification includes digital platforms designed to receive information from other digital platforms (col. 4, lines 45-65).

Referring to Claim 9:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses producing of the shared secret key comprises: analyzing contents of an incoming key selection vector (col. 5, line 55 – col. 6, line 12); and performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector (Ibid).

Referring to Claim 10:

Lotspiech in view of Liu discloses the limitations as discussed in Claim 9 above. Lotspiech further discloses the producing of the shared secret key further comprises: performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector (col. 6, lines 34-40).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
7/26/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100